Reasonable Skepticism Required

Comments on
"A Framework for Evaluating Process/Transaction-Level and Information Technology General Control Exceptions and Deficiencies Version 2, 21 October, 2005" in light of the Public Company Accounting Oversight Board (PCAOB) proposed auditing standard, "An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements" ("AS5")

Chris Anderson, CA(NZ), CISA, CMC, CISSP
Toronto, Canada, 8 May, 2007

The views presented in this document are the author's alone and do not claim to represent the views of any other organization.

On December 20, 2004, a working group of representatives from the major accounting firms in the U.S.A. outlined a suggested framework for evaluating manual and automated process/ transaction level, and information technology general control ("ITGC") exceptions and deficiencies, in the context of 'AUDITING STANDARD No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements' issued March 9, 2004 by the Public Company Accounting Oversight Board. While the Introduction to this framework document cautioned readers that 'the mere mechanical application of this framework will not, in and of itself, necessarily lead to an appropriate conclusion', it uses unproven logic to provide guidance to auditors that could lead to increased audit sampling risk and non-sampling risk, particularly when complex information systems are being evaluated by audit teams lacking appropriate experience and expertise. This aspect of the framework should not be adopted by regulatory and standards setting bodies without debate, since it sets the stage for liberal assessment of internal controls over financial reporting.

This paper looks at whether the changes from AS2 to the draft AS5 provides better direction to 'integrated auditors' on how to incorporate ITGC deficiencies into evaluation of internal control design.

In summary, the 'framework' appears to allow the auditor to evaluate ITGC as not designed effectively, but ignore the evidence of such a pervasive internal control deficiency when evaluating business cycle and associated application level internal control design effectiveness. Further, the requirement to expand the nature and extent of testing application controls in a weak IT general controls environment is merely an 'additional consideration' at the end of the section titled "Evaluating ITGC Deficiencies" (Chart 3). This could result in a situation where the nature and extent of application control testing for the purposes of evaluating the operational effectiveness of internal controls over financial reporting will be based on an optimistic but incorrect assessment of a) the expected number of internal control deviations in the IT general controls population, and b) the confidence that can be placed on the compliance test results. The auditor will also be able to conduct 'point-in-time' tests of business cycle/ application level internal controls in a period before a client's year-end (or required reporting date), and use the results of such tests as a basis for concluding on internal control operational effectiveness at year-end (or the reporting date). This removes the expectation that auditors apply 'reasonable skepticism' in conducting their control risk assessments.

The framework was incorporated into PCAOB 'Staff Questions and Answers – Auditing Internal Control Over Financial Reporting' issued November 22, 2004. Question Q35 of this document makes the following claim:

> *"IT general controls, by their nature, do not affect a company's financial statements directly."*

This premise is not supported by any explanation of the logic behind the statement or empirical evidence.

Answer A35 states:

> *"To evaluate the significance of a deficiency in IT general controls, the effect of the deficiency on application controls should be evaluated. An application control might be effective even if deficiencies exist in IT general controls. For example, in the presence of deficient program change controls, management and the auditor might be able to determine*

> *that, in the circumstances, the relevant application controls were operating effectively as of the date of management's assessment……In this case, the deficiency in IT general controls could be classified as only a deficiency. On the other hand, deficient program change controls might result in unauthorized changes to application controls, in which case the application controls are ineffective……..An IT general control deficiency in the absence of an application control deficiency could be classified as only a control deficiency."*

Automated controls need a 'safe house' within which to operate! If proper evaluation of internal control design effectiveness requires that the identified control is not only correctly designed on paper but *placed in operation*, then where else is an application control 'placed' if not into what we used to call a 'computer environment'? The conceptual and practical problem lies in the situation where apparently strong application controls operate in a weakly controlled computer environment, for example were accounting system packages are installed on a computer server within a LAN where the LAN and server operating system and database management system password rules are weak, little or no logging and review of possible unauthorized activity takes place and too many people have LAN and server administration privileges. This actually happens in small to medium organizations, and in a few large ones from time to time!.

Application controls do not operate in a vacuum. An operating system has to translate the application instructions into machine instructions, perform arithmetic and logic tasks, and provide the result back to the application. It is not logical to say that an application control continued to operate effectively even for 24 hours (e.g the date of management's assessment) where the organization has weak program change controls. In order for management, and the auditor, to have sufficient appropriate evidence that a specific application function supporting a control objective was designed effectively (including 'placed in operation') and operating effectively, either: a) the application software and all supporting system software has to be shown to have been frozen for at least the reporting date in question and then tested by management and the auditor in that 24 hours, or the whole system frozen for longer to accommodate the required testing; or b) the extent of testing performed by management and the auditor should be extensive enough to support the claim that the application control operated effectively as of the assessment date in an

environment that was not well managed and potentially hostile (i.e. not adequately protected from erroreous and malicious actions). Further, what extent of application control testing is sufficient to conclude that weak program controls did not cause application controls to stop operating correctly? If we have weak change controls that apply to the majority of a client's systems, just how much testing, and how rigorous a test plan is needed?

The CICA IT Control Guidelines (3rd Edition) clearly disagrees with the approach suggested by the working group in the 'evaluation framework': '*For reliance by management or auditors to be placed on fully automated control procedures or computer-assisted control procedures, general computer controls must be implemented and operating consistently and reliably. If they are not, there can be no assurance that fully automated and computer-assisted controls continue to operate as designed. Fully automated and computer –assisted controls do not compensate for weak general computer controls. If the condition of general computer controls is less than satisfactory, greater assurance must be sought from manual control procedures which do not in turn require assurance from general computer controls.'*

In July, 2004, the CICA Information Technology Advisory Committee issued a white paper titled 'IT Control Assessments in the context of CEO/CFO Certification'. It states: "IT controls are fundamental to the reliability and integrity of the information processed by the automated systems on which most organizations are dependent for their business and financial transaction processing – and overlooking or minimizing their importance creates a significant risk. ……The effectiveness of other controls, particularly manual controls, is also more often than not dependent on the effectiveness of IT controls."

The proposed AS5 provides better, but not ideal, guidance on how the risk that application controls will or will not function with a high level of processing integrity should be evaluated. However, it does not specifically require that an application based internal control be situated within a 'well controlled' computer environment for it to be considered designed effectively. Again, where an application control should be *placed* in

operation seems to have not been considered. What AS5 says that is relevant to this important issue is:

AS5 Extract	**Commentary**
4. The general standards …. require … professional skepticism.	To blithely evaluate the design of an application control without considering the controls over the computing environment it has been placed is the antithesis of skepticism
5. The auditor should use the same suitable, recognized control framework to perform his or her audit of internal control over financial reporting as management uses for its annual evaluation of the effectiveness of the company's internal control over financial reporting.	The widely used COSO framework does not specifically address the relationship between application controls and ITGCs.
12. …. A smaller and less complex company with simple business processes and centralized accounting operations often has relatively simple information systems that make greater use of off-the-shelf packaged software without modification. In the areas in which off-the-shelf software is used, the auditor's testing of information technology controls should focus on the application controls built into the pre-packaged software that management relies on to achieve its control objectives and the IT general controls that are important to the effective operation of those application controls.	This section leads one to consider the risk that application controls will not operate effectively without strong ITGC. If an application control is not going to operate effectively because of weak ITGC, how can it be evaluate as designed effectively?
34. For each significant process identified,	The flow of transactions within an

the auditor should…..Understand the flow of major classes of transactions, including how these transactions are initiated, authorized, processed and recorded;	application system obviously includes not only the compiled or run-time application logic and data but also the loading of the application logic into the CPU by the operating system and the manipulation of the associated data within say a database management system. We can't just conveniently state that this flow within the computer does not occur.
35. … Paragraphs .16 through .20, .30 through .32, and .77 through .79, of AU sec. 319, Consideration of Internal Control in a Financial Statement Audit, discuss the effect of information technology on internal control over financial reporting and the risks the auditor should assess. The auditor should apply this direction when auditing internal control over financial reporting.	See below for specific comments on AU sec. 319.
52. Factors that affect the risk associated with a control include…..The degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls);	For application controls, there is direct risk/reliance on ITGC.
62. In determining the extent of procedures to perform, the auditor should assess the following factors:…….Frequency of operation. Generally, the more frequently a manual control operates, the more operations of the control the auditor should	If the logic concerning a 'test of one' is sound, then it also follows that an 'automated control' has to be tested extensively in the absence of ITGC operating effectiveness. In fact, it is difficult to argue that such testing should

test to obtain sufficient evidence. Note: Testing a single operation of an automated control might result in sufficient evidence that the control operated effectively, provided that relevant information technology general controls also are operating effectively.	not be anything less than at a substantive extent if program change and access controls are not effective.

Above, S35 refers to AU sec. 319, Consideration of Internal Control in a Financial Statement Audit. The following sub-sections provide clear guidance that ITGC risks need to be considered when evaluating the design effectiveness of application controls:

- 19 IT also poses specific risks to an entity's internal control, including—
  - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
  - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
  - Unauthorized changes to data in master files.
  - Unauthorized changes to systems or programs.
  - Failure to make necessary changes to systems or programs.
  - Inappropriate manual intervention.
  - Potential loss of data.

- 20 The extent and nature of these risks to internal control vary depending on the nature and characteristics of the entity's information system. For example, multiple users, either external or internal, may access a common database of information that affects financial reporting. In such circumstances, a lack of control at a single user entry point might compromise the security of the entire database, potentially resulting in improper changes to or destruction of data. When IT personnel or users are given, or can gain, access privileges beyond those necessary to perform their assigned duties, a breakdown in segregation of duties can occur. This could result in unauthorized transactions or changes to programs or data that affect the financial statements. Therefore, the nature and characteristics of an entity's use of IT in its information system affect the entity's internal control

- 44 Application controls may be performed by IT (for example, automated reconciliation of subsystems) or by individuals. When application controls are performed by people interacting with IT, they may be referred to as user controls. The effectiveness of user controls, such as reviews of computer-produced exception reports or other information produced by IT,may depend on the accuracy of the information produced. For example, a user may review an exception report to identify credit sales over a customer's authorized credit limit without performing procedures to verify its accuracy. In such cases, the effectiveness of the user control (that is, the review of the exception report) depends on both the effectiveness of the user review and the accuracy of the information in the report produced by IT.

So, it is necessary to evaluate the possibility that application controls did not function as at the reporting date. By evaluating the general computer controls to be ineffective, we can not then deem application controls to have had a reasonable probability of continuing to function in a consistent manner, even for a day! Thus any attempt to execute compliance testing of an application control in a poorly controlled information systems environment is not logical. At worst, any compliance testing of application controls in a weak IT GC environment should be based on sampling extents that anticipate more than a limited number of errors, so that a 'considerable' level of assurance can be obtained from the results. Given that automated application controls related to 'regular' transaction processing are exercised thousands, if not millions, of times per day, then (conceptually at least) the auditor has the opportunity to test application controls extensively around, or at the reporting date, or the whole reporting period. The extent of testing of application controls in a poorly controlled information systems environment should not assume a low number of errors since the auditor has evidence that controls relevant to assessing the risk of operating effectiveness are inadequate. To ignore any likelihood that an application control will not be operating effectively when planning the compliance test extent is a fundamental departure from GAAS and commonly accepted threat/ risk assessment principles. Appendix B provides a summary of the Clark-Wilson model which explained these concepts in 1987. Thankfully AU sec.319 now leads us to a holistic understanding of IT controls and risks within integrated audits.

Thus, the control evaluation and test plan procedures should ensure that the automated internal control is not compromised by unauthorized changes to the programming code

directly performing the control function or other unauthorized code changes or data changes elsewhere in the application system or supporting infrastructure (eg database management systems, 'middleware').

The nature and extent of application control testing should be extensive in a situation where ITGC are not effective. AS2 paragraph 83 requires the auditor to evaluate:

- 'Whether there have been changes in the design of controls' when identifying controls to test'
- 'The degree to which the control relies on the effectiveness of other controls (for example, the control environment or information technology controls).'
- 'The complexity of the control'.

Unless the client has adequate controls over changes to systems, the auditor may not be able to determine, with sufficient assurance, the population of changes made to systems, some or all of which represent changes in the design and operation of controls. With millions of lines of code on each employees' desktop, and even more lines of code in server applications, operating systems, database management systems, and network elements such as routers and firewalls, the conservative auditor should conclude that the majority of application controls are very complex, and thus ensure that robust tests of their functioning are planned and executed that do not assume a low level of complexity, or ignore the control risks presented by a weakly controlled IT processing environment.

When planning application controls testing in a weak ITGC environment, the auditor should also not assume that the application controls are processing in a well managed and 'non-hostile' environment. AS2 paragraph 134 requires the auditor to 'evaluate how the controls interact with other controls' when evaluating the likelihood that misstatements could occur, and notes that 'there are other controls, such as information technology general controls, on which other controls depend.' AS2 paragraph 135 notes that the 'volume of activity in the account balance or class of transactions exposed to the deficiency' is a factor in determining the magnitude of the misstatement that could result from a control deficiency. If ITGCs are weak, then in most client situations, all

transactions were processed in a weak IT environment, and thus the 'magnitude' is the whole set of financial statements.

Allowing this 'framework' to continue to applied as it stands it may lead to inconsistent or liberal evaluation of internal controls over financial reporting, resulting in unacceptable audit risk, or inappropriate application of AS2 in 'borderline' situations. A client could have weak control over changes to systems and access to data, and the auditor could still attempt to conclude that internal controls are operating effectively as at the 'assessment date' across the major business cycles and supporting applications and be prepared to attest to this based on limited testing of the operational effectiveness of application controls. The client can merely 'promise' to fix these deficiencies, and even demonstrate some progress over time, and the auditor will be able to conclude that Governance is effective since senior management are 'working on it', and thus fundamental IT general control flaws will be relegated to internal control 'deficiencies'. The 'framework' could be seen by management and audit teams, without support from experienced and conservative IT auditors, to make the requirement to evaluate the IT General Controls toothless since auditors could argue that weak IT General Controls do not require any increase in compliance testing extents for automated (application) internal controls, there is no consequence of paying lip service to this high risk area or just not performing any work at all.

I suggest that, as corporations increase their reliance on automation, and particularly internetworking, that just the opposite of the above 'unfortunate series of events' needs to be promoted by regulatory bodies, and other stakeholders. Indeed, looking to Governance by management and the audit committee to fix this over time as a governance salve, is going to be found inappropriate as e-business increase the potential number of users in an organisation's systems that are not subject to the Governance measures within the corporation, such as physical security, salary reward mechanisms and the threat of being fired!

General Bibliography

- CICA IT GC Guidelines
- The External Audit, by Rod Anderson
- Extent of Audit Testing – a Research Study, CICA
- European Spreadsheet Risks Interest Group, http://www.eusprig.org/index.htm
- CICA Information Technology Advisory Committee: IT Control Assessments in the context of CEO/CFO Certification
- David D. Clark and David R. Wilson "A Comparison of Commercial and Military Computer Security Policies." IEEE Symposium of Security and Privacy, 1987, pages 184-194.

Appendix A
A Summary of
"A Comparison of Commercial and Military Computer Security Policies"

In 1987, this paper compared and contrasted commercial and military security policies and mechanisms and presented the following 'security policy valid in many commercial situations': "no user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted" and observed that "there are two mechanisms at the heart of fraud and error controls: the well-formed transaction and segregation of duty among employees. The concept of the well-formed transaction is that a user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of that data……The second mechanism to control fraud and error, segregation of duty, attempts to ensure the external consistency of the data objects: the correspondence between the data object and the real world object in represents." Clark and Wilson proposed that this correspondence is indirectly ensured by separating operations within a well-formed transaction and requiring people to execute the operations, and proposed that "to ensure that data items are manipulated only by means of well-formed transactions, it is first necessary to ensure that a data item can be manipulated only by a specific set of programs……control must be provided on the ability to install and modify these programs so that continued validity is ensured". Clark and Wilson identified the requirement that "the user of the system should not, by any sequence of operations, be able to modify the list of programs permitted to manipulate a particular data item or to modify the list of users permitted to execute a given program. If the individual user could do so, then there would be no control over the ability of an untrustworthy user to alter the system for fraudulent ends".

Clark and Wilson proposed the following commercial evaluation criteria:

- The system must separately authenticate and identify every user, so that his actions can be controlled and audited;

- The system must ensure that specified data items can be manipulated only by a restricted set of programs, and the data center controls must ensure that these programs meet the well-formed transaction rule
- The system must associate with each user a valid set of programs to be run, and the data center controls must ensure that these sets meet the segregation of duty rule;
- The system must maintain an auditing log that records every program executed and the name of the authorizing user
- The computer system must contain mechanisms to ensure that the system enforces its requirements;
- The mechanisms in the system must be protected against tampering or unauthorized change.

Of special note, Clark and Wilson pointed out that the last two criteria "which ensure that the system actually does what it asserts it does, are clearly an integral part of any security policy."